无后台服务器的射频识别标签安全查询协议

周景贤*①② 李 昊③ 周亚建①② 李国友①② 张 淼①②
①(北京邮电大学信息安全中心 北京 100876)
②(灾备技术国家工程实验室 北京 100876)
③(电子信息控制重点实验室 成都 610036)

摘 要：在许多射频识别(RFID)应用中，经常需要在多个标签中确定某个特定标签是否存在。在这种环境下，标签查询协议必不可少。然而，已有的协议要么存在安全漏洞，要么查询效率低下。利用 Hash 函数和时间戳，提出一个无后台服务器的 RFID 标签查询协议。GNY 逻辑被用于证明新协议的正确性。分析显示提出的协议可以高效的实现特定标签的查询，且能够抵抗一些主要攻击，实现对标签隐私的保护。

关键词：射频识别；查询协议；GNY 逻辑；追踪攻击
中图分类号：TP391 **文献标识码**： A **文章编号**：1009-5896(2012)11-2582-05
DOI: 10.3724/SP.J.1146.2012.00610

Server-less Radio Frequency Identification Tag Secure Searching Protocols

Zhou Jing-xian①② Li Hao③ Zhou Ya-jian①② Li Guo-you①② Zhang Miao①②
①(*Information Security Center*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
②(*National Engineering Laboratory for Disaster Backup and Recovery*, *Beijing* 100876, *China*)
③(*Science and Technology on Electronic Control Laboratory*, *Chengdu* 610036, *China*)

Abstract: Radio Frequency IDentification (RFID) tag search protocols are used in a situation where an reader finds a specific tag among multiple tags, which play important roles in many RFID applications. However, the existing protocols either have security weaknesses or exhibit poor efficiency. In this paper, a server-less RFID tag secure search protocol is proposed, which utilizes hash function and timestamp. GNY logic is used to prove its correctness. Analysis shows that presented protocol can be used to search a particular tag efficiently, and preserve tag's privacy against all major attacks.

Key words: Radio Frequency IDentification (RFID); Search protocol; GNY logic; Track attack

1 引言

RFID 应答器(transponders)、读取器、软体与服务市场在 2011 年增长了 9 亿美元，根据研究机构 ABI Research 预测，该市场未来 5 年可取得年平均 20%的增长率，到 2017 年可实现营收额 705 亿美元，那时 RFID 装置将无处不在。但是，由于存储和计算能力受限等先天缺陷，使得用户在享受 RFID 带来便捷的同时，也面临种种安全和隐私问题。例如，2007 年 2 月在 RSA 安全大会上，一家名为 IOActive 的公司展示了一款 RFID 克隆器，它可以复制信用卡去窃取密码。目前，学术界和工业界对 RFID 系统及其应用的安全问题已经进行了深入的研究，并取得了许多令人鼓舞的成果。不可否认，仍然有不少需要改进的地方。本文集中于对 RFID 标签查询安全协议的研究。

安全查询协议是一个 RFID 密码协议，按照协议交互，验证者(读写器)可以准确地判断某一特定标签是否存在于多个标签中，并且协议的攻击者得不到任何有用信息。例如，在 RFID 标签化图书的图书馆环境中，可以使用此类协议去查询一本可能丢失的图书是否还在。

2008 年，Tan 等人[1] 首次讨论了 RFID 查询机制，并给出了一系列标签查询协议。他们协议都采用挑战-响应机制，读写器首先广播一个请求消息，根据这个请求，如果目标标签存在，它将回复被加密的身份信息，区域内的其他标签以一定概率回复一个随机值。随后，一些研究成果相继被提出[2–10]。Kulseng 等人[2]基于线性反馈移位寄存器(LFSR)和物理不可克隆函数(PUF)，提出了几个轻量级安全

2012-05-18 收到，2012-08-22 改回
北京邮电大学青年科研创新计划专项(BUPT2011RC0212)和国家自然科学基金(60972077, 61070204, 61003285)资助课题
*通信作者：周景贤 zjxlr@yahoo.cn

查询协议，适用于低成本标签。Chao 等人[3]对这几个协议分析后发现，它们均不能抵抗标签追踪攻击。Kim 等人[4]提出了一个基于标签群身份的查询协议。他们将标签划分为多个群，每个标签只属于一个群，每个群有一个统一的群身份。在阅读器发布请求信息后，除了目标标签回复外，目标标签所在的群中每个标签都需要回复。然后由读写器验证所有的回复，以确定目标标签是否存在。类似于文献[1]使用的概率性回复一样，它的缺点是：为了查询一个标签，读写器需要进行大量的计算。文献[5]基于 Hash 函数给出了一个轻量级标签查询协议，作者们声称该协议计算代价小、且安全性高。然而，Lee 等人[6]分析指出，文献[1,5]提出的查询协议不能抵抗标签假冒攻击。在文献[6]中一个改进协议也被提出，但它沿用概率性回复策略去抵抗追踪攻击，这限制了该协议的扩展性。文献[7,8]的作者们分别提出了基于密钥更新的安全增强查询协议，但读写器和目标标签密钥更新不同步问题却没有得到有效解决。直接导致的后果就是：一次查询失败，之后所有的查询均不成功。文献[9]基于比特记录提出了一个前向安全的标签查询协议，然而协议的安全分析显示，它不能抵抗标签追踪攻击。文献[10]的突出贡献是：首先研究了标签查询协议的匿名安全性，但该文提出协议的安全完全依赖于第三方的诚实度，读写器变成仅仅转发信息的中继器，该协议的使用范围受到限制。

本文利用时间戳和 Hash 函数，提出一个新的标签查询协议，它不需要后台服务器的参与，适用于移动 RFID 环境。主要贡献包括：(1)形式化安全证明。用 GNY 逻辑证明新协议的正确性；(2)效率高。查询协议计算复杂度为：$O(1)$; (3)适用于低成本标签。协议仅采用 Hash 函数来保证数据传输的安全。

2　RFID 系统模型

传统的RFID系统由3个主体构成：标签(Tag)、读写器(Reader)和后台服务器。后台服务器往往是一个固定站，存储所有标签的信息，具有强大的计算能力，读写器通过有线的方式和服务器相连。该系统广泛地应用于超市购物、物流仓储管理等环境中。然而在现实中，后台服务器在给RFID系统带来便捷的同时也引入了一些新的问题，如：它与读写器之间的安全、可靠、持续的连接如何保证，易引起灾难性后果的服务器失效如何防止等。

本文研究的标签查询协议应用于无后台服务器的移动RFID系统，它是由阅读器 R 和一个标签集合组成。阅读器 R 是一个手持式移动装置，如：掌上电脑(PDA)等，它利用无线射频信号与标签进行通信，具有较强的计算和存储能力，可以独立对标签进行认证和查询。标签一般分为两类：有源(主动)标签和无源(被动)标签。我们主要考虑最为常用的被动标签，每个标签每次和一个阅读器进行通信。该系统适用于无法将服务器与读写器连接的远距离操作环境中；或标签分布范围较广，需要读写器频繁移动的环境中。

与传统RFID系统一样，在无后台服务器的RFID系统中，阅读器与标签之间是无线通信，容易遭受许多恶意攻击。我们假设攻击者可以截获标签和阅读器之间所有的通信信息，并且攻击者还可以对这些消息内容进行修改。特别地，在标签查询过程中，针对标签安全和隐私的攻击主要包括：窃听、冒充、重放、标签追踪和拒绝服务等。在第5节将对查询协议的安全性进行分析，这里不再赘述。

3　RFID 标签查询协议

在本节，我们提出一个使用在无后台服务器的 RFID 系统中的标签查询协议。协议参与主体有：读写器 R_i 和一个标签集合，其中假设 T_j 为目标查询标签。查询协议包括两个阶段：参数初始化阶段和标签查询阶段。图 1 给出了具体查询协议交互流程。

3.1　符号说明

文中需要用到的一些符号被列出在表 1 中。

表 1　符号描述

符号	描述
R_i , r_i	r_i 是用来定义 RFID 读写器 R_i 的身份
T_i , id_i	长度为 l bit 的 id_i 是用来定义 RFID 标签 T_i 的身份
S	安全可信的后台数据库
k_i	T_i 和 S 的共享密钥
$h(\cdot)$, $f(\cdot)$, l	$h(\cdot)$ 和 $f(\cdot)$ 是两个安全输出值长度为 l 的单向 Hash 函数， $h(\cdot), f(\cdot): \{0,1\}^* \to \{0,1\}^l$
L_i	R_i 从 S 下载关于标签的信息列表
$\mathrm{time}_{\mathrm{old}}$	标签之前存储的时间戳
$\mathrm{time}_{\mathrm{new}}$	本次会话使用的时间戳

3.2　初始化阶段

在初始化阶段，标签 T_i 被写入一个 l 长的唯一身份 id_i 和一个与 S 共享的密钥 k_i。读写器 R_i 有一个唯一的身份 r_i 和包含标签秘密信息的访问列表 L_i。r_i 和 L_i 是 R_i 向 S 成功认证自己后，从 S 处获取。其中，访问列表 $L_i \equiv \{(\mathrm{id}_1, h(r_i,k_1)),(\mathrm{id}_2, h(r_i,k_2)),\cdots,(\mathrm{id}_n, h(r_i,k_n))\}$。

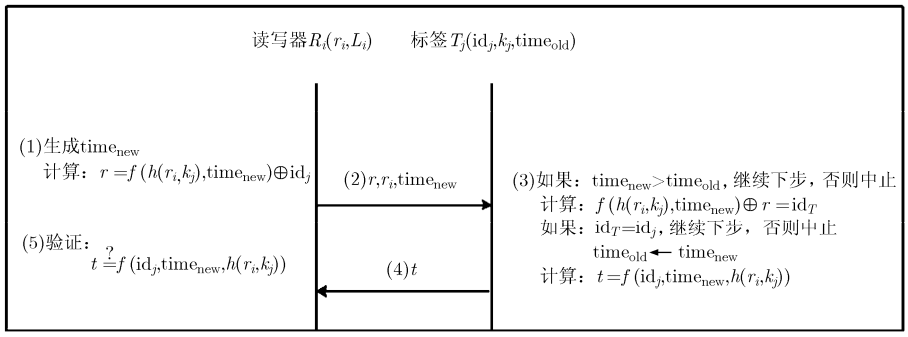

图 1 本文提出的协议交互流程

3.3 标签查询阶段

假设 R_i 想查询标签 T_j 是否存在，R_i 执行下列步骤去查询该标签：

(1) R_i 首先生成一个新的时间戳 $\mathrm{time}_{\mathrm{new}}$，并且计算值 r；

(2) R_i 广播 $r,r_i,\mathrm{time}_{\mathrm{new}}$ 给可达范围内的所有标签；

(3)收到查询请求之后，所有标签 T^* 首先验证 $\mathrm{time}_{\mathrm{new}}$ 是否大于 $\mathrm{time}_{\mathrm{old}}$。如果大于，它们利用自己的密钥 k_j 计算 $f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})$ 的值，然后检查 $f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})\oplus r$ 是否等于它的身份值 id_j。如果相等，那么它就是本次要寻找的标签。然后 T_j 计算值 t，并且替换 $\mathrm{time}_{\mathrm{old}}$ 为 $\mathrm{time}_{\mathrm{new}}$；

(4) T_j 回复消息 t 给 R_i；

(5) R_i 利用 $\mathrm{time}_{\mathrm{new}}$ 验证消息 t 的有效性。

4 协议的 GNY 逻辑分析

形式化方法的价值在于：能够发现安全协议中以前不为所知的漏洞。GNY 逻辑是一种形式化分析工具，在 1990 年由 Gong 等人[11]提出。GNY 逻辑是由 BAN 逻辑发展而来的，与 BAN 逻辑相比，它具有更强的表现能力和适应性。目前，它被认为是影响最大的一种 BAN 类逻辑之一。

为了验证协议的安全性，我们利用 GNY 逻辑对协议的目标，假设和消息传递进行形式化分析，证明从协议的假设出发，经过协议的运行可以达到预先设定的目标。证明过程中使用的逻辑规则都来自于文献[11]。为了简化证明过程，我们直接给出逻辑规则代码。希望进一步研究的读者，可以参见文献[11]。

4.1 协议的假设、目标及其形式化

(1)关于标签 T_j 的假设：T_j 拥有身份信息 id_j，两个单向 Hash 函数 $h(\cdot),f(\cdot)$；拥有秘密信息 k_j；协议双方验证的依据是拥有共同秘密值 $h(r_i,k_j)$，所以 T_j 相信它与 R_i 共享 $h(r_i,k_j)$；T_j 相信 $\mathrm{time}_{\mathrm{new}}$ 是新鲜的，否则协议不能成功运行。

标签的假设可以形式化为：$T_j \ni \mathrm{id}_j$，$T_j \ni h(\cdot)$，$f(\cdot),T_j \ni k_j,T_j| \equiv T_j \xleftrightarrow{h(r_i,k_j)} R_i,T_j| \equiv \#(\mathrm{time}_{\mathrm{new}})$。

(2)关于读写器 R_i 的假设：R_i 拥有身份信息 r_i，单向函数 $f(\cdot)$；R_i 拥有关于 T_j 的秘密消息 $h(r_i,k_j)$，并且在协议运行中发送自己的身份 r_i 给 T_j，所以 R_i 相信它和 T_j 共享信息 $h(r_i,k_j)$；R_i 相信 $\mathrm{time}_{\mathrm{new}}$ 是新鲜的。

读写器的假设可以形式化为：$R_i \ni r_i, R_i \ni f(\cdot)$，$R_i| \equiv R_i \xleftrightarrow{h(r_i,k_j)} T_j$，$R_i| \equiv \#(\mathrm{time}_{\mathrm{new}})$。

(3)协议的目标：作为一种自动查询技术，经过安全协议的运行，目标标签 T_j 能够相信挑战信息是来自于合法的读写器 R_i，并且以前未被使用，也就是新鲜的；同样协议运行后，读写器 R_i 也能够确认收到的回复信息来自于目标标签 T_j，并且是新鲜的。

协议目标可以形式化为

(1) $T_j| \equiv R_i| \sim \#(f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})\oplus \mathrm{id}_j, r_i, \mathrm{time}_{\mathrm{new}})$

(2) $R_i| \equiv T_j| \sim \#(f(\mathrm{id}_j,\mathrm{time}_{\mathrm{new}},h(r_i,k_j)))$

4.2 形式化分析

在明确了协议的假设、目标后，我们可以利用 GNY 逻辑中的相关推理规则，证明协议能够从假设出发，经协议运行后达到预先设定的目标。

图 1 中的(2)可 GNY 逻辑形式化为

$$T_j \lhd {}^*(f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})\oplus \mathrm{id}_j, r_i, \mathrm{time}_{\mathrm{new}}) \sim\sim R_i| \equiv T_j \ni h(r_i,k_j)$$

显然有：$T_j \lhd r_i$，由 GNY 推理规则 $P1$ 可得：$T_j \ni r_i$；由前提假设条件 $T_j \ni k_j, T_j \ni h(\cdot)$ 成立，根据 GNY 推理规则 $P4$ 可得：$T_j \ni h(r_i,k_j)$。

根据协议可知 $T_j| \equiv \phi(f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})\oplus id_j, r_i,\mathrm{time}_{\mathrm{new}})$ 和 $T_j| \equiv \otimes(T_j)$ 成立，根据 GNY 推理规则 $I1'$ 可得：$T_j| \equiv R_i| \sim (f(h(r_i,k_j),\mathrm{time}_{\mathrm{new}})\oplus \mathrm{id}_j, r_i, \mathrm{time}_{\mathrm{new}})$。

由假设 $T_j| \equiv \#(\mathrm{time}_{\mathrm{new}})$，根据 GNY 推理规则

$F1$ 可得：$T_j \mid\equiv \#(f(h(r_i,k_j),\text{time}_{\text{new}}) \oplus \text{id}_j, r_i, \text{time}_{\text{new}})$。所以目标(1) $T_j \mid\equiv R_i \mid \sim \#(f(h(r_i,k_j), \text{time}_{\text{new}}) \oplus \text{id}_j, r_i, \text{time}_{\text{new}})$ 成立。

图 1 中的(4)可 GNY 逻辑形式化为

$$R_i \lhd {}^*f(\text{id}_j, \text{time}_{\text{new}}, h(r_i,k_j))$$

为证明目标(2)，类似于以上的方法，应用 GNY 逻辑规则 $I1'$ 可以证明：$R_i \mid \equiv T_j \mid \sim (f(\text{id}_j, \text{time}_{\text{new}}, h(r_i,k_j)))$，应用 GNY 逻辑规则 $F1$ 可以证明：$R_i \mid \equiv \#(f(\text{id}_j, \text{time}_{\text{new}}, h(r_i,k_j)))$。

所以目标(2) $R_i \mid \equiv T_j \mid \sim \#(f(\text{id}_j, \text{time}_{\text{new}}, h(r_i, k_j)))$ 成立。

可见，通过协议的运行，该协议可以在前提假设的基础上实现预定的设计目标。

5　协议的安全性及效率分析

与许多形式化逻辑一样，GNY 逻辑也有其不足之处。比如：无详细的时间概念，无否定形式等。所以，某些潜在攻击仅仅依靠 GNY 逻辑无法被发现(比如：窃听攻击，追踪攻击等)。本节将从安全性能和实施效率两方面来对提出的标签查询协议进行分析。

5.1 协议安全性分析

本文主要从：标签追踪、窃听、拒绝服务、冒充欺骗和重放攻击 5 个方面来分析新协议的安全。

(1)窃听攻击：攻击者 A 可以通过窃听 R_i 和 T_j 之间的不安全信道，收集到消息：$r, r_i, \text{time}_{\text{new}}, t$。显然对于攻击者 A 来说这些值没有任何意义。time_{new} 是随机值；r_i 是代表读写器的身份，攻击者可以通过它来知道是哪个读写器，但对于追踪目标标签没有任何帮助。$f(\cdot)$ 是单向函数，所以 A 通过 r 也不能获得比随机数更多的信息。

注：r_i 的明文传输，确实泄漏了读写器 R_i 的身份，但本文讨论的追踪攻击对象是查询目标标签。同时要想实现身份信息的秘密传输，只有加密算法可以做到。为保证所提协议的轻量级，我们并不考虑加密算法的使用。

(2)冒充攻击：由于 $h(r_i,k_j)$ 和 k_j 的机密性，同时根据第 4 节的形式化证明可以知道，如果 $r, r_i, \text{time}_{\text{new}}$ 和 t 能通过验证，就可以说明对方是合法的。也就是说，在提出的协议中，公开传输值有任何改动导致不匹配，就会引起协议失败，冒充攻击是不可能成功的。

(3)重放攻击：本文提出的协议中，采用时间戳 time_{new} 来抵抗重放攻击。重放以前的消息必然导致时间戳验证不能通过，引起协议的失败。所以，重放攻击对本协议不构成威胁。

注：由于标签的低成本和计算能力的限制，放置同步时钟是不可能的。所以我们采用在标签内存储时间戳的方式，比较条件为 $\text{time}_{\text{new}} > \text{time}_{\text{old}}$，认证成功则实施 $\text{time}_{\text{new}} \to \text{time}_{\text{old}}$ 操作；否则不变。

(4)拒绝服务攻击：拒绝服务攻击一般是指攻击者试图实施中间人攻击，为了引起 R_i 和 T_j 之间秘密值不同步，导致以后协议交互的失败。但是，在我们提出的协议中，R_i 和 T_j 在每次会话中，不需要进行密钥更新。因此，本文协议能安全抵抗拒绝服务攻击。

(5)标签追踪攻击：追踪就是攻击者能将 T_j 与其它标签区分开来。攻击者有两种方式来实现对目标标签 T_j 的追踪。(a)窃听 R_i 和 T_j 之间的所有通信；(b)利用窃听到的信息，对 T_j 实施重放攻击。对于第 1 种攻击，我们的协议是安全的，因为攻击者不可能每次都能预测到时间戳 time_{new} 和 T_j 的回复值 t。因此，攻击者不能将 T_j 与其它标签进行区分；在另一种攻击中，攻击者可能窃听到了 R_i 和 T_j 之间一次通信的查询挑战和响应，然后攻击者重复广播查询挑战。由于时间戳的使用，使得 T_j 不会对攻击者的挑战做出回应。

从以上讨论的关于安全的 5 个方面，我们将提出的协议与文献[1]，文献[7]，文献[6]的协议进行比较(表 2)。通过比较可以发现，我们的协议具有最好的安全性质，是唯一满足了所有安全需求的协议。

表 2 协议安全性比较

	文献[1]	文献[6]	文献[7]	本文的协议
抗窃听攻击	√	√	√	√
抗冒充攻击	×	√	√	√
抗重放攻击	×	×	√	√
抗拒绝服务攻击	×	×	×	√
抗追踪攻击	√	√	√	√

5.2 协议效率分析

标签查询系统中有两类实体：标签和读写器，所以在效率方面我们主要考虑：查询协议的交互轮数、单个标签的计算量和读写器的计算量 3 部分。文献[1]和文献[6]使用概率性回复来抵抗标签追踪攻击，使得读写器的计算量与标签数成正比，查询效率较低。文献[7]采用加密算法和密钥更新的方法，来实现协议的安全。对标签的计算能力和硬件都提出了很高的要求。我们提出的协议采用简单的 2 轮交互认证，对于每次查询读写器只需要 2 次 Hash 运算。

表 3 总结了我们提出协议的效率，其中，C_H 为一次 Hash 运算的计算花费；C_E 为一次加密运算的

表 3 协议效率比较

	文献[1]	文献[6]	文献[7]	本文的协议
交互轮数	2	3	2	2
标签计算量	$2C_H$	$3C_H$	$2C_H + 2C_E$	$3C_H$
读写器计算量	$1 + N \cdot \lambda / 2C_H$	$1 + N \cdot \lambda / 2C_H$	$2C_H + 3C_E$	$2C_H$

计算花费；N 为标签总个数；λ 为标签回复概率值。通过比较可以发现，在 4 个标签查询协议中，我们的协议是计算代价要求最低的。

6 结束语

本文首先对标签查询问题的研究现状进行了分析，然后提出了一个无后台服务器的 RFID 标签查询协议。GNY 逻辑分析表明，从该协议的假设出发经协议运行可以达到预先设定的协议目标。分析显示，本文提出的协议在满足各种安全需求的同时，具有很高的运行效率。同时，由于标签仅需要一个 Hash 函数电路来实现隐私保护，成本较低，更适用于资源紧张的无源标签。协议应用场合可以是在图书馆进行图书查询，也可以是在奢侈品零售店进行商品查询。

然而，目前所提出的标签查询协议，基本上都是以标签的身份作为查询依据，使得这些协议只能用于一对一的环境中。如果一个读写器想一次查询满足某一条件的所有标签是否存在，那么目前的协议无法直接使用。所以，下一步研究内容是一对多的标签查询协议机制和基于某些特征的标签查询机制。

参 考 文 献

[1] Tan C C, Sheng B, and Li Q. Secure and serverless RFID authentication and search protocols[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(4): 1400–1407.

[2] Kulseng L, Yu Z, Wei Y, *et al*.. Lightweight secure search protocols for low-cost RFID systems[C]. Proceedings of the 29th IEEE International Conference on Distributed Computing Systems, IEEE Computer Society, Washington, DC, USA, 2009: 40–48.

[3] Chao L, Li H, Ma J F, *et al*.. Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems [J]. *International Journal of Radio Frequency Identification Technology and Applications*, 2012, 1(4): 3–12.

[4] Kim Z, Kim J, Kim K, *et al*.. Untraceable and serverless RFID authentication and search protocols[C]. 2011 Ninth IEEE International Symposium on Busan, Parallel and Distributed Processing with Applications Workshops (ISPAW), Montreal, Canada, 2011: 278–283.

[5] Lin I C, Tsaur S C, and Chang K P. Lightweight and server-less RFID authentication and search protocol [C]. Proceedings of the 2009 Second International Conference on Computer and Electrical Engineering, IEEE, New York, 2009, 2: 95–99.

[6] Lee C F, Chien H Y, and Laih C S. Server-less RFID authentication and searching protocol with enhanced security [J]. *International Journal of Communication Syst*em, 2012, 25(3): 376–385.

[7] Zuo Y J. Secure and private search protocols for RFID systems[J]. *Information System Front* , 2010, 12(5): 507–519.

[8] 曹峥, 邓淼磊. 通用可组合的 RFID 搜索协议[J]. 华中科技大学学报(自然科学版), 2011, 39(4): 56–59.
Cao Z and Deng M L. Universally composable search protocol for RFID[J]. *Journal of Huazhong University of Science and Technology* (*Natural Science Edition*), 2011, 39(4): 56–59.

[9] Hoque M E, Rahman F, and Ahamed S L. S-search: finding RFID tags using scalable and secure search protocol[C]. Proceedings of the 2010 ACM Symposium on Applied Computing (SAC), Sierre, Switzerland, 2010: 439–443.

[10] Yoon H S and Youm H Y. An anonymous search protocol for RFID systems[J]. *Journal of Convergence Information Technology*, 2011, 8(6): 44–50.

[11] Gong L, Needham R, and Yahalom R. Reasoning about belief in cryptographic protocols[C]. Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, Oakland, California, 1990: 234–248.

周景贤： 男，1981 年生，博士生，研究方向为移动通信安全、RFID 系统安全.

李 昊： 男，1979 年生，博士，研究方向为电子对抗、网络对抗.

周亚建： 男，1971 年生，副教授，研究方向为网络安全、密码学.

李国友： 男，1983 年生，博士生，研究方向为移动网络安全、网络编码学.

张 淼： 男，1980 年生，讲师，研究方向为可信计算、终端安全.